WE CLAIM:

1. A secure access transceiver for providing secure and authenticated access to command controllable computerized equipment, comprising:

means for establishing a carrier signal in response to an access request from a remote entity seeking access to the equipment from a remote point;

means for authenticating the entity seeking access to the computerized equipment; and

means for enabling data to pass through the secure access transceiver to the computerized equipment only upon authentication of the entity seeking access to the computerized equipment and for preventing data from passing through the secure access transceiver.

2. A secure access transceiver as claimed in claim 1, wherein the means for authentication is of an embedded electronics type.

3. A secure access transceiver as claimed in claim 1, wherein the means for authentication is of a removable electronics type, such as a daughter card or a smart card.

4. A secure access transceiver as claimed in claim 1, wherein the means for authenticating the entity seeking access to the computerized equipment further comprises means for storing and retrieving information to enable the storage and retrieval of authentication

information, transaction records and authentication information revocation lists.

5. A secure access transceiver as claimed in claim 4, wherein the means for authentication further comprises an absolute time clock to enable a validity of the authentication information to be restricted to specified periods of time.

6. A secure access transceiver as claimed in claim 5, wherein associated with the transaction records is a maximum number of transactions enabled to trigger a critical event when the maximum number of transactions have been performed by the remote entity.

7. A secure access transceiver as claimed in claim 6, wherein the critical event triggers a transaction record dump to a known remote point.

8. A secure access transceiver as claimed in claim 1, wherein the means for enabling data to pass through to the computerized equipment is a signal enabling a shift in/out clock controlling data transfer to the computerized equipment.

9. A secure access transceiver as claimed in claim 1, wherein the means for enabling data to pass through to the computerized equipment is a signal enabling a read function which enables the data to be read from a register holding data to be transferred to the computerized equipment.

10. A method of providing authenticated access to command controllable computerized equipment connected to a secure access transceiver in response to an access request from an entity at a remote point comprising the steps of:

performing an initial handshake sequence;

interrupting the handshake sequence upon carrier detection;

exchanging authentication information between the entity at the remote point and the secure access transceiver;

validating the authentication information; and

enabling data to pass through the secure access transceiver to the computerized equipment for a duration of a service session upon successful authentication and otherwise preventing data from passing through the secure access transceiver to the computerized equipment.

11. A method as claimed in claim 10 wherein prior to the step of performing an initial handshake, a data port of the secure access transceiver connected to the computer equipment is disabled to ensure that access to the command controllable computer equipment is denied before authentication information is validated.

12. A method as claimed in claim 10 wherein the step of validating authentication information comprises the steps of:

generating a segment of data at the secure access transceiver and sending the segment of data in a message to the remote point;

encrypting the segment of data at the remote point and sending the encrypted segment of data in a message back to the secure access transceiver; and

decrypting the encrypted segment of data and comparing the decrypted segment of data with the segment of data sent thereby to validate that the remote point is authorized to access the computerized equipment.

13. A method as claimed in claim 12 wherein the method further comprises the steps of:

digitally signing the encrypted segment of data at the remote point before sending the encrypted segment of data to the secure access transceiver; and

verifying the digital signature to ensure that the remote point is authorized to access the computerized equipment before decrypting the encrypted segment of data.

14. A method as claimed in claim 12 wherein at least one electronic access key is issued by a service co-ordination center enforcing network centric-control of access to the controlled computerized equipment.

15. A method as claimed in claim 14 wherein the service co-ordination center assigns the remote point in response to an access request to at least one maintenance project and at least one electronic access key is assigned to the remote point for the project.

16. A method as claimed in claim 15 wherein the service co-ordination center updates the secure access transceiver with at least one electronic access key after the remote point has been assigned to a project.

17. A method as claimed in claim 16 wherein the at least one electronic access key is revoked after the project is terminated, or the remote point is removed from the list of authorized entities assigned to the project.

18. A method as claimed in claim 17 wherein revoked electronic access keys are added to a revocation list of the secure access transceiver that is updated by the service co-ordination center.

19. A method as claimed in claim 18 wherein the service co-ordination center accesses the secure access transceiver for administration purposes, the secure access transceiver permitting administrative changes to be effected only after verification of authentication information for administration purposes.

20. A method of enforcing network-centric control over access to a plurality of command controllable computerized equipment units accessed through secure access transceivers comprising the steps of:

defining a project and storing a project definition along with project parameters in a project database;

assigning at least one user the project;

issuing at least one electronic access key to the user assigned to the project; and

updating a secure access transceiver for accessing computerized equipment associated with the project with a corresponding electronic access key;

whereby the secure access transceiver uses the corresponding electronic access key to authenticate the user when the user requests access to the computerized equipment.

21. A method as claimed in claim 20 wherein the electronic access key is valid for only one access session to the computerized equipment, and the user is required to authenticate to the service co-ordination center and receive an electronic access key before requesting access to the computerized equipment.

22. A method as claimed in claim 20 wherein the electronic access key is issued to the user for a duration of the project and the user uses the electronic access key to access to the computerized equipment as required during a lifetime of the project.

23. A method as claimed in claim 20, wherein the service co-ordination center stores a copy of the electronic key in the project database, and the authentication server and the secure access transceivers maintain a revocation list of invalid and expired electronic access keys.

24. A method as claimed in claim 23, wherein the electronic access key issued to the user and the corresponding electronic access key have an associated life term and on expiration of the life term the electronic access keys are written to the revocation lists.

25. A method as claimed in claim 20 wherein the step of updating a secure access transceiver comprises the steps of:

establishing a communications session between an authentication server and the secure access transceiver;

validating to the secure access transceiver that the authentication server is a trusted administrator;

commencing an administration session with the secure access transceiver; and

electronic access key in a memory of the secure access transceiver.

26. A method as claimed in claim 25 wherein the step of validating to the secure access transceiver that the authentication server is a trusted administrator comprises the steps of:

receiving authentication information from the authentication server;

validating the authentication information to ensure that the authentication server is a trusted administration authority; and

accepting data to be stored in the memory only if the authentication server is validated as a trusted administration authority.

27. A method as claimed in claim 26 wherein validating the authentication information comprises the steps of:

receiving from the authentication server a certificate signed by a certification authority;

verifying that the validity of the certificate and dropping the communications session in an instance when the certificate is invalid;

generating a segment of data and sending the segment of data to the authentication server;

receiving the segment of data returned from the authentication server in an encrypted form and decrypting the encrypted segment of data using an electronic administration access key; and

comparing the decrypted segment of data to a copy of the segment of data, and dropping the communications session in an instance when the segment of data do not match.

28. A method as claimed in claim 27 wherein the segment of data is a random number.

29. A method as claimed in claim 27 wherein the electronic administration access key used by the secure access transceiver is an embedded key that cannot be read or changed by a party accessing the secure access transceiver using a dial-up connection.

30. A method as claimed in claim 29 wherein the electronic administration access key is stored on a smart card or a daughter card that cannot be read by the party accessing the secure access transceiver using the dial-up connection.

31. A secure access controller for providing secure authenticated access to command controllable computerized equipment, comprising:

means for establishing a communications link in response to an access request from an entity seeking access to the computerized equipment from a remote point;

means for authenticating the entity seeking access to the computerized equipment; and

means for enabling data to pass through the secure access controller to the equipment only upon authentication of the entity seeking access to the computerized equipment and otherwise preventing data from passing through the secure access controller.

32. A secure access controller as claimed in claim 31, wherein the means for authentication is of an embedded electronics type.

33. A secure access controller as claimed in claim 31, wherein the means for authentication is of a removable electronics type, such as a daughter card or a smart card.

34. A secure access controller as claimed in claim 31, wherein the means for authenticating the entity seeking access to the computerized equipment further comprises means for storing and retrieving information to enable the storage and retrieval of authentication information, transaction records and authentication information revocation lists.

35. A secure access controller as claimed in claim 34, wherein the means for authentication further comprises an absolute time clock to enable a validity of the authentication information to be restricted to specified periods of time.

36. A secure access controller as claimed in claim 35, wherein associated with the transaction records is a maximum number of transactions permitted to trigger a critical event when the maximum number of transactions have been performed by the remote entity.

37. A secure access controller as claimed in claim 36, wherein the critical event triggers a transaction record dump to a known remote point.

38. A secure access controller as claimed in claim 31, wherein the means for enabling data to pass through to the computerized equipment is a signal enabling a shift in/out clock controlling data transfer to the computerized equipment.

39. A secure access controller as claimed in claim 31, wherein the means for enabling data to pass through to the computerized equipment is a signal enabling a read function which enables the data to be read from a register holding data to be transferred to the computerized equipment.

40. A method of providing authenticated access to command controllable computerized equipment connected to a secure access controller in response to an access request from an entity at a remote point comprising the steps of:

detecting a communications link established through an access transceiver to the secure access controller;

receiving authentication information through the communications link from the entity at the remote point;

validating the authentication information to determine if the entity is authorized to access the computerized equipment; and

enabling data to pass through the secure access controller to the computerized equipment for a duration of a service session upon successful authentication, and otherwise preventing data from passing through the secure access controller to the command controllable computerized equipment.

41. A method as claimed in claim 40 wherein a data port to the computerized equipment is normally disabled to ensure that commands cannot be passed through to the

computerized equipment before authentication information is validated.

42. A method as claimed in claim 40 wherein the step of validating the authentication information comprises the steps of:

generating a segment of data at the secure access controller and sending the segment of data in a message to the entity at the remote point;

encrypting the segment of data at the remote point and sending the encrypted segment of data in a message back to the secure access controller; and

decrypting the encrypted segment of data and comparing the decrypted information string with the segment of data sent to ensure that the remote point is authorized to access the computerized equipment.

43. A method as claimed in claim 42 wherein the method further comprises the steps of:

digitally signing the encrypted segment of data at the remote point before sending the encrypted segment of data to the secure access controller; and

verifying the digital signature to ensure that the remote point is authorized to access the computerized equipment before decrypting the encrypted segment of data.

44. A method as claimed in claim 42 wherein electronic access keys are issued by a service co-ordination center that is responsible for ensuring

that only authorized entities have access to the computerized equipment.

45. A method as claimed in claim 44 wherein the service co-ordination center assigns a user at the remote point to at least one project, and at least one electronic access key set is assigned to the user for the project.

46. A method as claimed in claim 45 wherein the service co-ordination center issues the electronic access key to the user at the remote point and issues a corresponding electronic access key to the secure access controller after the user at the remote point has been assigned to a project.

47. A method as claimed in claim 46 wherein the electronic access key is revoked after the project is terminated, and the user is removed from the list of authorized entities assigned to the project.

48. A method as claimed in claim 47 wherein the electronic access key is revoked by adding the corresponding electronic access key to a key revocation list that is updated in the secure access controller by the service co-ordination center.

49. A method as claimed in claim 48 wherein the service co-ordination center accesses the secure access controller using an electronic access key set for administration purposes, the secure access controller

permitting administrative changes to be effected only after the validation of authentication information for administration purposes.

50. A method of enforcing network-centric control over access to a plurality of a command controllable computerized equipment units accessed through a secure access controllers comprising the steps of:

defining a project and storing a project definition along with project parameters in a project database;

assigning at least one to user the project;

issuing at least one electronic access key to the user assigned to the project; and

updating the secure access controller for accessing computerized equipment associated with the project with a corresponding electronic access key;

whereby the secure access controller uses the corresponding electronic access key to authenticate the user when the user requests access to the computerized equipment.

51. A method as claimed in claim 50 wherein the electronic access key is valid for only one access session to the computerized equipment, and the user is required to authenticate to the service co-ordination center and receive an electronic access key before requesting access to the computerized equipment.

52. A method as claimed in claim 50 wherein the electronic access key is issued to the user for a

duration of the project and the user uses the electronic access key to access to the computerized equipment as required during a life of the project.

53. A method as claimed in claim 50, wherein the service co-ordination center stores a copy of the electronic access key pair in the project database and the authentication server and the secure access controller maintain a revocation list of invalid and expired electronic access keys.

54. A method as claimed in claim 53, wherein the electronic access key issued to the user and the corresponding electronic access key have an associated life term and on expiration of the life term the electronic access keys are written to the revocation list.

55. A method as claimed in claim 20 wherein the step of updating a secure access controller comprises the steps of:

establishing a communications session between an authentication server and the secure access controller;

validating to the secure access controller that the authentication server is a trusted administrator;

commencing an administration session with the secure access controller; and

storing the corresponding electronic access key in a memory of the secure access controller.

56. A method as claimed in claim 55 wherein the step of validating to the secure access controller that the authentication server is a trusted administrator comprises the steps of:

receiving authentication information from the authentication server;

validating the authentication information to ensure that the authentication server is a trusted administration authority; and

accepting data to be stored in the memory only if the authentication server is validated as a trusted administration authority.

57. A method as claimed in claim 56 wherein validating the authentication information comprises the steps of:

receiving from the authentication server a certificate signed by a certification authority;

verifying that the validity of the certificate;

generating a segment of data and sending the segment of data to the authentication server;

receiving the information string returned from the authentication server in an encrypted form and decrypting the encrypted information string using an electronic administration access key; and

comparing the decrypted segment of data to a copy of the segment of data sent.

58. A method as claimed in claim 57 wherein the segment of data is a random number.

59. A method as claimed in claim 57 wherein the electronic administration access key used by the secure access server is an embedded key that cannot be read or changed by a user accessing the secure access controller using a dial-up connection.

60. A method as claimed in claim 29 wherein the electronic administration access key is stored on a smart card or a daughter card that cannot be read by the user accessing the secure access controller using the dial-up connection.